

5 preguntas para hacerle a tu proveedor de mitigación de DDoS

A medida que aumentan la frecuencia y la complejidad de los ataques DDoS, resulta fundamental seleccionar el servicio de mitigación de DDoS adecuado para proteger tus redes y usuarios. Sin embargo, no todos los servicios se crean de la misma forma, y elegir el incorrecto puede provocar dolores de cabeza, tiempo de inactividad y problemas de rendimiento inesperados.

Estas son cinco preguntas que debes tener en cuenta al evaluar a los proveedores de servicios de mitigación de DDoS:

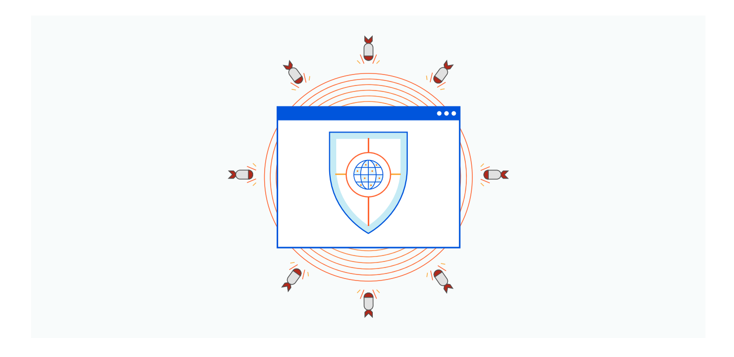
1. ¿El servicio es nativo de la nube?

Para que un servicio de mitigación de DDoS sea eficaz, debe ser nativo de la nube, y no un producto de tecnología local que se haya virtualizado y alojado en centros de datos en la nube. ¿Cuál es la diferencia? Los servicios de mitigación nativos de la nube pueden escalarse sin problemas en función de las necesidades de tu empresa sin provocar cuellos de botella artificiales en el rendimiento, mientras que los dispositivos virtuales alojados en la nube aún conllevan la complejidad administrativa que implica el hardware local.



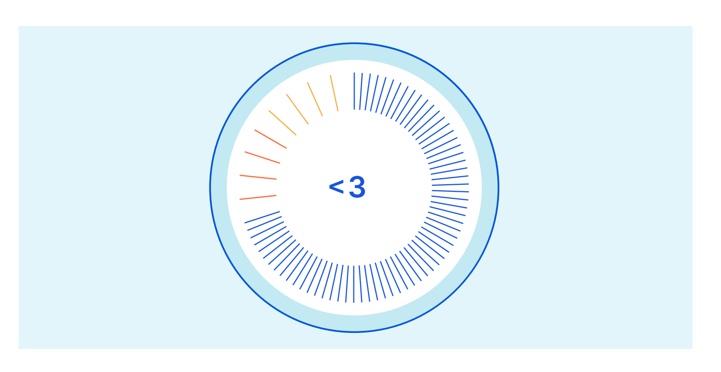
2. ¿Cuánta capacidad de red ofrece el proveedor?

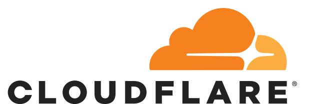
Los ataques DDoS a gran escala, como el ataque de 2,3 Tbps que tuvo como objetivo un cliente de AWS en 2020, pueden sobrepasar a los proveedores de servicios que no tienen la capacidad de red suficiente para absorber el tráfico DDoS. A fin de combatir ataques a esta escala, elige un proveedor que ofrezca suficiente capacidad de red para resistir ataques sin causar tiempo de inactividad ni reducciones de rendimiento.



3. ¿Con qué rapidez puede el servicio detectar ataques DDoS y reaccionar ante ellos?

Frente a un ataque, es fundamental que el tiempo de mitigación (lo que se tarda en detectar y mitigar los ataques) sea lo más corto posible. Cualquier solución que provoque más de unos segundos de tiempo de inactividad podría causar daños irreversibles a la experiencia del cliente, a la reputación de la marca y a los ingresos.





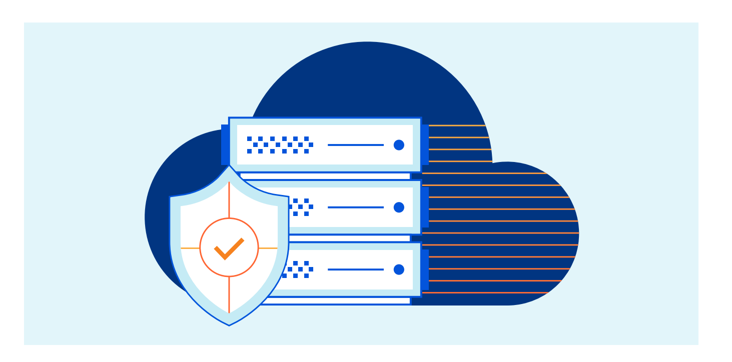
4. ¿El servicio está disponible en todos los centros de datos?

Cuando las funciones de depuración de DDoS no están disponibles en todos los centros de datos, el tráfico debe retroceder través de “centros de depuración” especializados que a menudo agregan latencia y afectan el rendimiento de la aplicación. Elige un proveedor que pueda ofrecer servicios de mitigación en todos los centros de datos mientras mantiene el tráfico en las rutas más eficaces.



5. ¿El servicio está automatizado?

Un servicio de mitigación de DDoS eficaz debe ofrecer capacidades de automatización y autoservicio desde un panel de control o API para que puedas activar y gestionar la protección contra amenazas de forma rápida. Busca un proveedor que sea fácil de contactar, que responda rápidamente y que sea proactivo en la detección de amenazas. Además, debe mitigar los ataques sin aumentar el tiempo de inactividad de tus servicios.



Magic Transit de Cloudflare protege subredes IP completas contra ataques DDoS y, al mismo tiempo, acelera el tráfico de la red. La red global de Cloudflare, que abarca centros de datos en más de 200 ubicaciones, bloquea un promedio de 70.000 millones de amenazas por día, incluidos algunos de los ataques DDoS más grandes de la historia.

Para comenzar a usar Magic Transit, solicita una demostración gratuita hoy mismo.